какого-либо фотона и затем этот же фотон будет переслан В, то в итоге количество ошибок намного увеличится, и это станет заметно Алисе. Это приведет к тому, что А и В будут полностью уверены в состоявшемся перехвате фотонов. Если расхождений нет, то биты, использованные для сравнения, отбрасываются, ключ принимается. С вероятностью $1-2^{-k}$ (где k — число сравненных битов) канал не прослушивался. Существует оценка, что если ошибка в канале меньше приблизительно 11%, то секретная передача данных возможна.

Квантовая криптография позволяют создавать системы, обеспечивающие практически 100%-ю защиту ключевой информации.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие для студ. – Минск: БГТУ, 2016. – 220 с.

2.Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович // Труды БГТУ. Серия VI. Физико-математические науки и информатика. – Минск: БГТУ. – 2005. – Вып.XIII.– С.161–164.

3. Лесовик Г. Б. Фундаментальные проблемы физики квантовых технологий. [Электронный ресурс]. – Режим доступа:

https://mipt.ru/education/chairs/fpfkt/downloads/edumaterials/presentations/presentation.pdf. – Дата доступа: 15.04.2019.

4. Wikipedia. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/BB8 - Дата доступа: 15.04.2019.

УДК 004.056

Студ. М. Н. Карпович, Е. В. Карпович
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ШИФРОВАНИЕ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ. УЯЗВИМОСТИ АЛГОРИТМА «РУКОПОЖАТИЯ»

Технология WPA является развитием технологий WEP [1]. Описать эту технологию можно с помощью формальной записи: WPA = 802.1X + EAP + TKIP +MIC, где 802.1X – набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне, EAP – расширяемый протокол аутентификации, TKIP – протокол целостности временного ключа, MIC – проверка целостности сообщений.

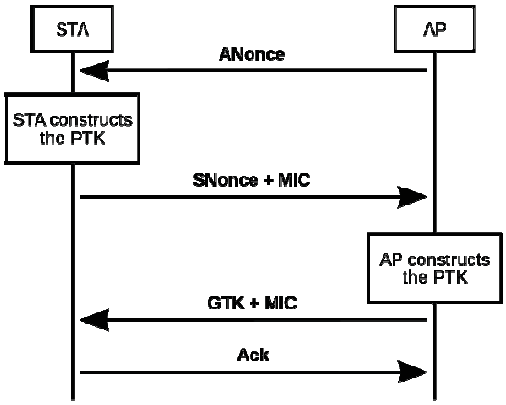


Рисунок 1 – Схема 4-х этапного «рукопожатия»

4-х этапное «рукопожатия» (рис. 1) работает следующим образом. Точка доступа (AP) отправляет клиенту (STA) временное значение PTK, в свою очередь использует Pre-SharedKey и пять других параметров — SSID, AuthenticatorNounce (ANounce или временное значение), SNounce, MAC-адрес точки доступа и MAC-адрес wifi-клиента. Этот ключ в дальнейшем использует шифрование между точкой доступа (AP) и wifi-клиентом.

Удалось на практике доказать, что злоумышленник способен заставить жертву сбрасывать счётчики путём повторной отправки сообщения 3-го этапа во время 4-х этапного «рукопожатия».

В обычной WPA/WPA2 PSK атаке по словарю, злоумышленник будет использовать словарь с программой. Программа будет выводить 256-bitPre-SharedKey для каждой парольной фразы и использовать ее с другими параметрами, которые были описаны в создании PTK. PTK будет использован для проверки MessageIntegrityCheck (MIC) в одном из пакетов 4-х этапного «рукопожатия». Если они совпадут, то парольная фраза в словаре будет верной, в противном случае неверной. Именно так работает WPA/WPA2 PSK. Нашей главной задачей будет выбор цели для получения доступа и перехват EAPOL пакетов, из которых впоследствии мы получим нужную нам информацию [2].

На рис.1-8 последовательно представлены скриншоты и скрипты, соответствующие отдельным шагам анализируемой технологии.

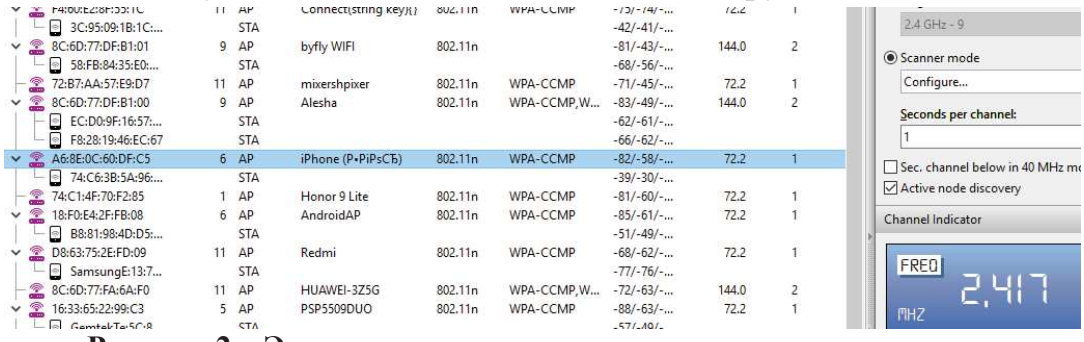


Рисунок 2 – Этап перевода адаптера в режим прослушивания, выбор нужного объекта

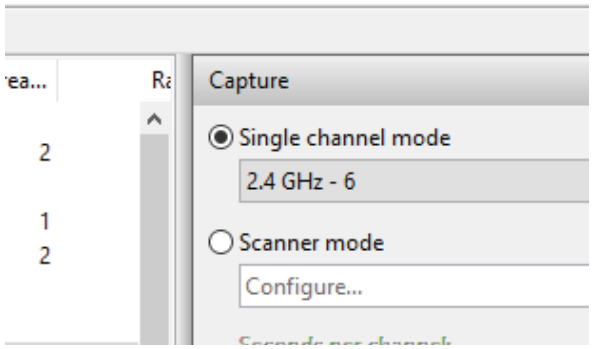
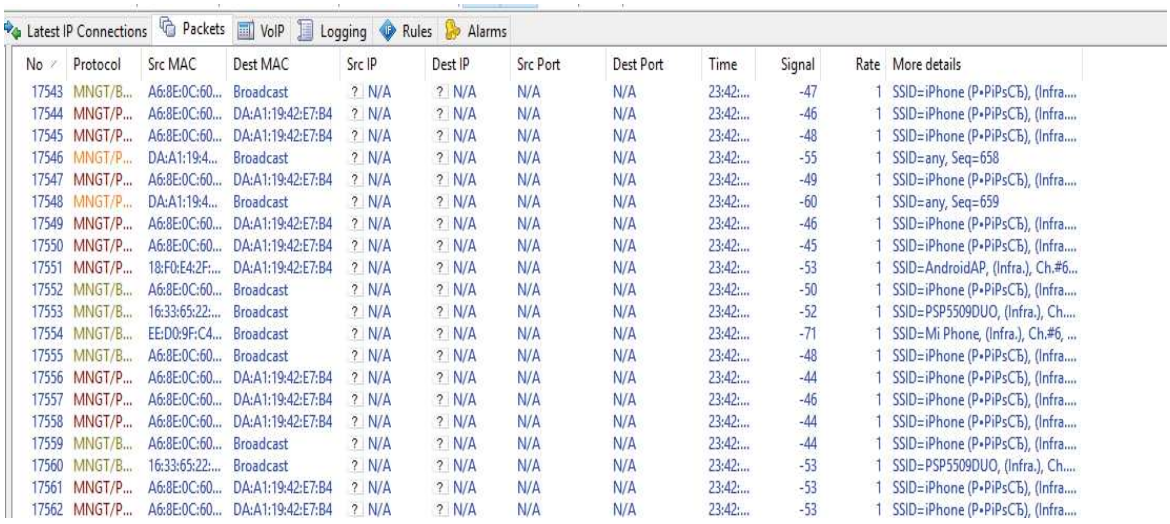


Рисунок 3 – Адаптер на прослушивание канала на котором находится объект

Программа предназначена для работы с дампами, содержащими пакеты для последующего взлома. Также она используется для:

- мониторинга: захват пакетов и экспорт данных в текстовые файлы для дальнейшей обработки сторонними инструментами,
- проведения атак: повторные атаки, деаутентификация, фальшивые точки доступа и другие через внедрение пакетов,
- тестирования: проверка WiFi-карт и возможностей драйвера (захват и внедрение),
- взлома: WEP и WPA PSK (WPA 1 и 2).

Для решения этой задачи были выпущены специальные «патчи» для операционных систем, а так же анонсированный в 2018 году WPA3. Он будет дополнен встроенной защитой от брутфорс-атак [2], индивидуальным шифрованием данных для усиления конфиденциальности пользователей в открытых Wi-Fi сетях, упрощенная настройка IoT-устройств, а так же усовершенствованный криптографический стандарт для сетей Wi-Fi, который будет иметь «192-разрядный пакет безопасности» [3].



No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest Port	Time	Signal	Rate	More details
17543	MNGT/B...	A6:8E:0C:60...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-47	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17544	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-46	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17545	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-48	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17546	MNGT/P...	DA:A1:19:4...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-55	1	SSID=any, Seq=658
17547	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-49	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17548	MNGT/P...	DA:A1:19:4...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-60	1	SSID=any, Seq=659
17549	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-46	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17550	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-45	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17551	MNGT/P...	18:F0:E4:2F:...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-53	1	SSID=AndroidAP, (Infra.), Ch.#6...
17552	MNGT/B...	A6:8E:0C:60...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-50	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17553	MNGT/B...	16:33:65:22:...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-52	1	SSID=PSP5509DUO, (Infra.), Ch....
17554	MNGT/B...	EE:D0:9F:C4...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-71	1	SSID=Mi Phone, (Infra.), Ch.#6, ...
17555	MNGT/B...	A6:8E:0C:60...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-48	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17556	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-44	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17557	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-46	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17558	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-44	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17559	MNGT/B...	A6:8E:0C:60...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-44	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17560	MNGT/B...	16:33:65:22:...	Broadcast	? N/A	? N/A	N/A	N/A	23:42:...	-53	1	SSID=PSP5509DUO, (Infra.), Ch....
17561	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-53	1	SSID=iPhone (P•PiPsCЂ), (Infra....
17562	MNGT/P...	A6:8E:0C:60...	DA:A1:19:42:E7:B4	? N/A	? N/A	N/A	N/A	23:42:...	-53	1	SSID=iPhone (P•PiPsCЂ), (Infra....

Рисунок 4 – Таблица полученных пакетов

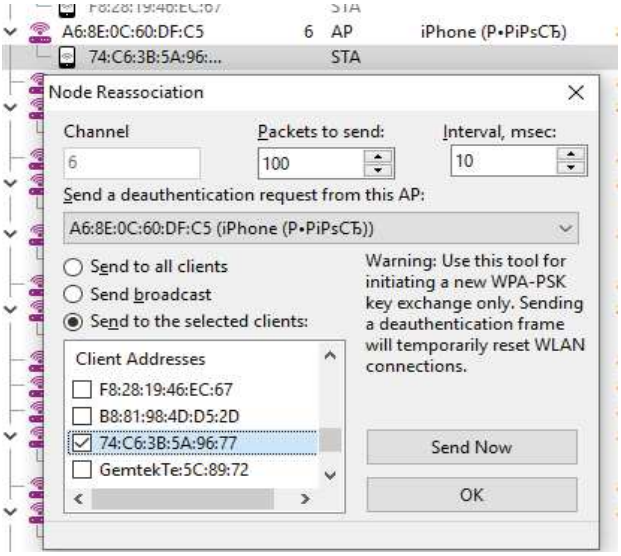


Рисунок 5 – Реассоциация узлов

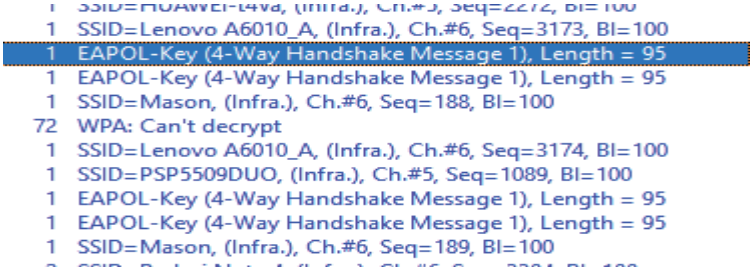


Рисунок 6 – Таблица EAPOL пакетов

Далее используется программа aircrack-ng GUI.

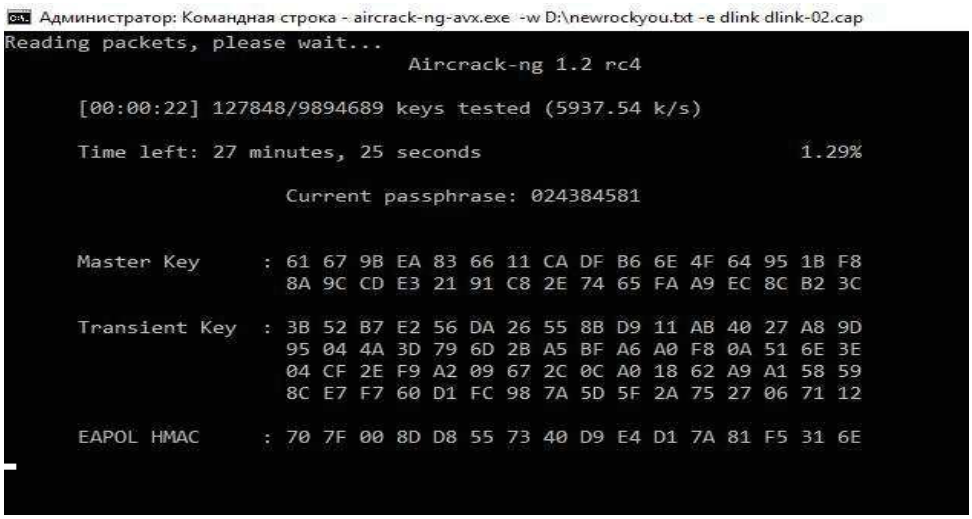


Рисунок 7 – Окно программы aircrack-ng

```
                    KEY FOUND! [ qwerty123 ]

Master Key     : ED FF 23 E4 68 76 CE C7 BA A3 49 9F 8E 3C 32 CD
                 44 96 43 9E DC 30 C7 5E 46 73 F0 40 CE 2B BE C8

Transcient Key : 7F 5E AD AE 34 94 39 AD AC 4E C5 64 B2 7B FE CF
                 28 CF F5 1D 64 AC 5B BA B5 CB F6 25 11 0B 3C F4
                 C1 A6 8B 85 E3 68 C1 97 27 4C 03 65 D1 67 E3 1E
                 67 22 1E 51 9A 6D 49 67 F6 5F BE 47 4A 7A D6 51

EAPOL HMAC     : 36 33 8C 56 61 C7 9C 93 9D 47 A4 B5 A4 1F 05 F4
```

Рисунок 8 – Результат успешного взлома

ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 399 с.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

3. Нефёдова, М. Анонсирован стандарт WPA3, Wi-Fi обещают сделать безопаснее / М. Нефёдова. [Электронный ресурс]. – Режим доступа: https://xakep.ru/2018/01/09/wap3/. – Дата доступа: 10.04.2019.

УДК004.056

Магистрант А. А. Сущеня
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ВНЕДРЕНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ В КОНТЕЙНЕР ФОРМАТА EPUB

Актуальность исследования стеганографии обострена проблемами защиты цифрового контента от несанкционированного использования. Ввиду этого существует необходимость расширения и углубления теоретической базы стеганографии как платформы для тайной передачи и хранения информации [1].

С развитием информационных технологий стали появляться цифровые объекты, имеющие в своей структуре избыточность, которую можно использовать для реализации стеганографических методов передачи данных. Одними из таких объектов являются электронные книги. На сегодняшний день, наиболее популярным форматом электронных книг являются EPUB. Рассмотрим структуру данного формата. EPUB — это ZIP-файл, сжатый особым образом. В этом можно